United Nations A/RES/73/27

General Assembly

Distr.: General
11 December 2018

Seventy-third session
Agenda item 96

Resolution adopted by the General Assembly on 5 December 2018

[*on the report of the First Committee (A/73/505)*]

73/27. Developments in the field of information and telecommunications in the context of international security

The General Assembly,

Recalling its resolutions 36/103 of 9 December 1981, 43/78 H of 7 December 1988, 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012, 68/243 of 27 December 2013, 69/28 of 2 December 2014, 70/237 of 23 December 2015 and 71/28 of 5 December 2016,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Underscoring the aspirations of the international community to the peaceful use of information and communications technologies (ICTs) for the common good of humankind and to further the sustainable development of all countries, irrespective of their scientific and technological development,

Noting that capacity-building is essential for cooperation of States and confidence-building in the field of ICT security,

Recognizing that some States may require assistance in their efforts to bridge the divide in the security of ICTs and their use,

Noting that providing assistance, upon request, to build capacity in the area of ICT security is essential for international security,

Affirming that capacity-building measures should seek to promote the use of ICTs for peaceful purposes,

18-21207 (E) 131218

Please recycle

Confirming that ICTs are dual-use technologies and can be used for both legitimate and malicious purposes,

Expressing concern that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in future conflicts between States is becoming more likely,

Stressing that it is in the interest of all States to promote the use of ICTs for peaceful purposes, with the objective of shaping a community of shared future for humankind in cyberspace, and that States also have an interest in preventing conflict arising from the use of ICTs,

Noting that the United Nations should play a leading role in promoting dialogue among Member States to develop common understandings on the security of and the use of ICTs, as well as in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour in this sphere, encourage regional efforts, promote confidence-building and transparency measures and support capacity-building and the dissemination of best practices,

Expressing concern that embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security,

Considering that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes,

Underlining the importance of respect for human rights and fundamental freedoms in the use of ICTs,

Welcoming the effective work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome reports transmitted by the Secretary-General,[1]

Welcoming also that, in considering the application of international law to State use of ICTs, the Group of Governmental Experts, in its 2015 report,[2] identified as of central importance the commitments of States to the following principles of the Charter of the United Nations and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States,

Confirming the conclusions of the Group of Governmental Experts, in its 2013[3] and 2015[2] reports, that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment, that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of ICTs can reduce risks to international peace, security and stability, and that, given the unique attributes of such technologies, additional norms can be developed over time,

---

[1] A/55/201, A/68/98 and A/70/174.

[2] A/70/174.

[3] A/68/98.

Confirming also that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory,

Reaffirming the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news, which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, cooperation and friendly relations among States and nations,

Recognizing the duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States,

Stressing that, while States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations,

1. *Welcomes* the following set of international rules, norms and principles of responsible behaviour of States, enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 2013[3] and 2015[2] adopted by consensus and recommended in resolution 71/28 entitled "Developments in the field of information and telecommunications in the context of international security", adopted by the General Assembly on 5 December 2016:

1.1. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

1.2. States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

1.3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts.

1.4. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

1.5. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 of 5 July 2012[4] and 26/13 of 26 June 2014[5] on the promotion, protection and enjoyment of human rights on the Internet, as well as

[4] See *Official Records of the General Assembly, Sixty-seventh Session, Supplement No. 53* and corrigendum (A/67/53 and A/67/53/Corr.1), chap. IV, sect. A.

[5] Ibid., *Sixty-ninth Session, Supplement No. 53* (A/69/53), chap. V, sect. A.

General Assembly resolutions 68/167 of 18 December 2013 and 69/166 of 18 December 2014 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

1.6. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

1.7. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

1.8. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

1.9. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products.

1.10. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

1.11. States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

1.12. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

1.13. States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behaviour in information space with regard to their potential role;

2. *Calls upon* Member States to promote further, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information;

3. *Considers* that the purpose of such measures could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems;

4. *Invites* all Member States, taking into account the assessments and recommendations contained in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,[1] to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

(b) Efforts taken at the national level to strengthen information security and promote international cooperation in this field;

(c) The content of the concepts mentioned in paragraph 3 above;

(d) Possible measures that could be taken by the international community to strengthen information security at the global level;

5. *Decides* to convene, beginning in 2019, with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent, an open-ended working group acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States listed in paragraph 1 above, and the ways for their implementation; if necessary, to introduce changes to them or elaborate additional rules of behaviour; to study the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations; and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building and the concepts referred to in paragraph 3 above, and to submit a report on the results of the study to the General Assembly at its seventy-fifth session, and to provide the possibility of holding, from within voluntary contributions, intersessional consultative meetings with the interested parties, namely business, non-governmental organizations and academia, to share views on the issues within the group's mandate;

6. *Also decides* that the open-ended working group shall hold its organizational session in June 2019 in order to agree on the organizational arrangements connected with the group;

7. *Further decides* to include in the provisional agenda of its seventy-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

45th plenary meeting
5 December 2018